VARSTVOSLOVJE,
letn. 18
št. 1
str. 84–97

Vpliv raznolikosti podatkov na odvzem in preiskovanje mobilnih naprav v organizacijah

Blaž Markelj, Igor Bernik

Namen prispevka:

Mobilne naprave so stičišče različnih podatkov, ki izhajajo iz osebne in poslovne rabe. Zaradi enostavnosti rabe in izjemnih možnosti povezovanja so se pojavile številne varnostne grožnje. Te pretijo uporabnikom mobilnih naprav in povečujejo tveganje informacijskovarnostnih incidentov. V primeru odtujitve poslovnih podatkov, ki so na mobilni napravi, in zahtev po preiskavi, ne moremo več govoriti o »običajnem« zasegu in pregledu mobilne naprave – varovati moramo osebne podatke in ravnati na pravno predpisan način ohranjanja pričakovane zasebnosti.

Metode:

Dognanja temeljijo na pregledu virov ter analizi in interpretaciji rezultatov dvostopenjske raziskave (anketa in intervju) med uporabniki mobilnih naprav v 34 slovenskih organizacijah. Anketirani so bili zaposleni, ki pri svojem delu uporabljajo informacijsko-komunikacijske tehnologije, intervjuvanci pa odgovorni za informacijsko varnost v obravnavanih organizacijah.

Ugotovitve:

Raziskava kaže, da je meja med osebno in poslovno rabo pri rabi mobilnih naprav izginila, ob stalnem povečevanju groženj se povečuje tudi tveganje incidentov (izguba informacij, odtujitve mobilne naprave ipd.). Za varno rabo mobilnih naprav je treba spoštovati zakonodajo, informacijskovarnostna pravila, politike in standarde, ki jasno določajo, kako uporabljati mobilno napravo v povezavi s poslovnimi podatki. Ob incidentu sta pomembna odziv posameznika in organizacije ter postopek obravnave in preiskovanja.

Omejitve:

Viri in primerljive raziskave, ki obravnavajo rabo mobilnih naprav, z njim povezane grožnje in varnostne incidente, so redki, organizacije pa ne prijavljajo tovrstnih incidentov.

Praktična uporabnost:

Mobilne naprave lahko zaradi varnostnih incidentov povzročijo škodo – tako uporabnikom kot organizacijam. Njihova raba pa predstavlja različna varnostna tveganja, predlagani so ukrepi za preprečevanje in obravnavo varnostnih incidentov.

Izvirnost:

Tematika o rabi mobilnih naprav v povezavi z varnostnimi incidenti je v začetni fazi razvoja, raziskave redke, predstavljene ugotovitve za slovenski prostor pa novost.

UDK: 004.056

Ključne besede: mobilne naprave, grožnje, tveganja, varnostni incidenti

The Impact of the Diversity of Information on the Seizure and Investigation of Mobile Devices in Organisations

Purpose:

Mobile devices carry various data originating from personal and business use of mobile devices. Due to their simple use and extreme possibilities of connecting, numerous security threats to mobile device users have arisen. These threats increase the risk of information security incidents. In case of loss of business data on mobile device, the seizure and inspection of a mobile device should be dealt in a specifically sensitive manner; personal data must be protected according to the reasonable expectation of privacy.

Design/Methods/Approach:

The results are based on the literature review, analysis and interpretation of results of a two-level research (survey and interview) among the users of mobile devices in 34 Slovenian organisations. The survey was conducted among the employees who use information communication technology with their work, whereas the interviewees were the ones who are responsible for information security in these organisations.

Findings:

The research shows that the boundary between personal and business use of mobile devices has disappeared and the constant rise of threats increases also the risk of security incidents (such as loss of data, loss of mobile device, etc.). In order to use mobile devices safely, respective legislation, rules of information security, politics and standards, which clearly define the appropriate use of mobile device in relation to business data, must be respected. When an incident does occur, the response of an individual and the organisation and the procedure of investigation are of importance.

Research Limitations/Implications:

Previous literature and similar researches, which deal with the use of mobile devices, connected threats and security incidents, are rare, whereas the organisations do not report such incidents.

Practical Implications:

Mobile devices can cause damage to the users and organisations via security incidents. Their use represents various security risks, therefore the article includes suggestions for prevention and dealing with security incidents.

Originality/Value:

The topic of using mobile devices in connection to security incidents is in the early stages of development, the research is rare and the findings are a novelty for Slovenia.

UDC: 004.056

Keywords: mobile devices, threats, risk, security incidents

1 UVOD

Kibernetski prostor predstavlja stičišče številnih informacij, ki so na različne načine povezane z elektronskimi napravami, med katere sodijo splošno uporabljane mobilne naprave[1]. Zaradi enostavnega upravljanja in dovršene tehnologije so mobilne naprave v zgolj nekaj letih postale stalni spremljevalec posameznika, tako v zasebne kot poslovne namene. Različna omrežja (npr. mobilna, WiFi, bluetooth, NFC), raznovrstna programska in strojna oprema so elementi, ki sestavljajo mobilno napravo in so že tako izpopolnjeni, da uporabniku dajejo optimalno uporabniško izkušnjo.

Zagotavljanje informacijske varnosti je bilo v preteklosti bolj preprosto. Eden od vzrokov je bila nemobilnost elektronskih naprav in direktnega, nadzorovanega fiksnega dostopa do podatkov. Mobilne naprave pa omogočajo stalno brezžično povezanost s kibernetskim prostorom in različne oddaljene dostope do podatkov. Tako s prehodom od statičnega, nemobilnega dela in uporabe naprav, za katere v vsakem trenutku vemo, kje se fizično nahajajo, in so običajno še dodatno fizično varovane, k dinamičnemu delu z mobilnimi napravami in povezavo s spremljajočo mobilno informacijsko tehnologijo (mobilna omrežja, brezžično povezovanje, razne aplikacije ...). Zaradi omenjene mobilnosti je zagotavljanje kibernetske varnosti drugače kot prej, večinoma pa mnogo zahtevnejše. Mobilne naprave so bolj izpostavljene, iz varovanih prostorov se selijo v javnost zato so bolj izpostavljene grožnjam, zlorabe pa pogostejše. V primeru zlorab mobilne naprave oziroma v primeru incidenta v povezavi z mobilno napravo je tudi pridobivanje in analiziranje dokazov zelo kompleksno. Ko se zloraba ali incident zgodi, je le-tega treba raziskati in preprečiti njegovo ponavljanje.

Posamezna mobilna naprava je polna raznovrstnih podatkov. Nekatere od teh omogoča zajemati naprava sama (fotografije, trenutna lokacija, pot gibanja ipd.), nekateri pa so v napravo preneseni preko različnih omrežij. Ti podatki so lahko osebne in/ali poslovne narave. Ker večina uporabnikov mobilno napravo potrebuje v poslovnem okolju za poslovno rabo in hkrati tudi za osebne potrebe, se je meja med osebnimi in poslovnimi podatki, ki so na posamezni mobilni

1 *Med mobilne naprave uvrščamo predvsem naprave, ki imajo prilagojene operacijske sisteme, kot so iOS, Android, BlackBerry OS ali Windows mobile, in so prenosljive (mobilni telefoni, tablični računalniki itd.). V to kategorijo se lahko uvrsti vse naprave, ki se lahko prenašajo in pri katerih je dostop v internet mogoč brez fizične povezave (tudi prenosniki, prenosne igralne konzole, industrijski čitalci itd.), medtem ko v skupino mobilnih telefonov spadajo tako mobilni telefoni, ki so namenjeni zgolj klicanju in pisanju kratkih sporočil, kot tudi pametni mobilni telefoni, ki predstavljajo sodobno komunikacijsko napravo, saj poleg klicanja prek mobilnih omrežij omogočajo še kopico dodatnih funkcij, ki so podobne funkcijam osebnega računalnika.*

napravi in do katerih z napravo dostopamo, zabrisala. To pa predstavlja velika informacijskovarnostna tveganja, kar dokazujeta McAfee (2014) in Juniper Networks (2013) v svojih poročilih, kjer hkrati navajata drastično povečanje groženj v zadnjih letih, ki lahko na različne načine zlorabijo podatke iz mobilne naprave in podatke, do katerih z njimi dostopamo. S tem namenom poročilo Ocena groženj resne in organizirane kriminalitete (angl. *Serious and Organised Crime Threat Assessment*) (Europol, 2013), ki ga je Europol pripravil za leto 2013, opredeljuje razvoj mobilnih naprav, možnost nenehne komunikacije ter razvoj škodljive programske opreme v prvi vrsti kot sredstvo, ki organizirani kriminaliteti omogoča širjenje kriminalnih mrež in razširja možnosti zlorab. Omenja hiter razvoj škodljive programske opreme za mobilne naprave, ki za kibernetsko kriminaliteto predstavlja možnost širjenja delovanja. To pa predstavlja nevarnost uporabnikom mobilnih naprav, poslovnim subjektom in družbi kot celoti. V primeru uresničitve grožnje je izrednega pomena, da uporabniki mobilnih naprav incident prijavijo ustreznim organom – policiji, CERT-u ter pooblaščenim osebam v organizaciji, ki morajo ustrezno izvesti postopek preiskave in zavarovati dokazno gradivo ne zgolj zaradi incidenta, pač pa tudi zaradi morebitne forenzične analize in ugotavljanja kazenske odgovornosti.

Prispevek predstavlja izhodišča obravnavane tematike, v nadaljevanju pa se naveže na rezultate raziskave, ki je bila izvedena med slovenskimi organizacijami. Raziskava je pokazatelj realnega stanja celovite rabe mobilnih naprav in virov ogrožanja, obenem pa rezultati kažejo na frekvenco uporabljenih storitev. Iz vrste uporabljenih storitev in groženj izhajajo tveganja, le-ta pa so podkrepljena z rezultati že uresničenih groženj. Raziskani so tudi postopki, načini in frekvence prijav varnostnih incidentov ustreznim organom in vpeljane zaščite, ki jih uporabniki mobilnih naprav uporabljajo kot sredstvo boja proti grožnjam in preprečevanja incidentov. Nujna in logična posledica uresničitve grožnje je preiskovanje vzrokov varnostnega incidenta in njegovih (možnih) posledic; tako znotraj organizacije kot tudi v eventualnem kazenskem postopku zoper uporabnika, še posebej v primeru evidentnih kršitev predpisanih postopkov varne uporabe mobilnih naprav. Tako so v prispevku opredeljeni postopki preiskovanja mobilnih naprav, ki so vezani na slovensko zakonodajo, v tem okviru pa poudarjamo pomen pravilnikov in standardov za varno rabo mobilnih naprav.

2 KIBERNETSKA VARNOST IN RABA MOBILNIH NAPRAV

Mobilne naprave so eden od najhitreje razvijajočih se segmentov informacijske tehnologije in sodobne družbe, zato so izjemno izpostavljene različnim grožnjam. Olavsrud (2013) navaja grožnje mobilnim napravam kot najhitreje razvijajoče se informacijske grožnje prihodnosti. Le-te razdela tudi poročilo Mednarodne organizacije za telekomunikacije (International Telecommunication Union [ITU], 2012), v katerem so nazorni opisi poznanih kibernetskih groženj in njihovih posledic. Skoraj vse navedene kibernetske grožnje pa lahko posredno ali neposredno ogrožajo mobilne naprave. Število mobilnih naprav, okuženih s škodljivo programsko opremo (angl. *malware*), konstantno narašča, narašča tudi število drugih, novih groženj mobilnim napravam, kar potrjujejo izčrpna poročila

o razširjenosti in smernicah razvoja groženj mobilnim napravam, ki so jih objavila podjetja F-Secure (2013), Gartner (2013), International Data Corporation [IDC] (2013), Juniper Networks (2013), Lookout (2011), McAfee (2014). Različni viri, kot npr. Bernik (2014), OWASP Mobile Security Project (Open Web Application Security Project [OWASP], 2013) in Deloitte (Norton, 2012), navajajo različne grožnje kibernetski varnosti ob rabi mobilnih naprav, kot so:

- izguba ali odtujitev mobilne naprave,
- tatvina podatkov (z različno izvedenimi napadi na napravo),
- napad na mobilno napravo s programsko opremo, ki ima varnostne vrzeli,
- prestrezanje podatkov oz. vdori v omrežja (omrežni komunikacijski kanali oz. uporaba nezavarovanih in neznanih omrežij WI-FI),
- sledenje (posledica nenadzorovanega oddajanja modula GPS ali identifikacije lokacije v omrežjih),
- prevzem nadzora nad mobilno napravo ter samodejno oddajanje podatkov (brez vednosti uporabnika),
- škodljiva programska oprema (*malware*, *spyware*, trojanski konji, virusi itn.),
- zloraba Bluetootha in NFC-ja (*bugging*, *snarfing*, *jacking*, *smacking).* In še bi lahko naštevali.

Dnevno se seznam dopolnjuje z novimi in novimi grožnjami (npr. ITU, 2012; McAfee, 2014), ki na svojevrsten način delujejo z namenom odtujitve podatkov, spremljanjem ali posegom v delovanje posameznika in organizacije.

3 VARNOSTNI INCIDENTI

Organizaciji Deloitte (Norton, 2012) in OWASP (2013) sta na podlagi analiz razmer na področju groženj mobilnim napravam in ob sodelovanju strokovnjakov s področja kibernetske varnosti izdelali seznam, ki prikazuje povečanje tveganj uresničitve groženj. Izhaja tako iz domneve o uporabi organizacijskega kot tehničnega vidika rešitev in ukrepov pri rabi mobilnih naprav. Tveganje za uresničitev grožnje izhaja tudi iz:

- pomanjkanja uradne strategije pri uvajanju in uporabi mobilnih naprav,
- premajhnega varnostnega nadzora mobilnih naprav s strani strokovnjakov za IT,
- slabo opredeljenega lastništva mobilne naprave in predvsem podatkov,
- strožjega nadzora nad uporabo mobilne naprave in
- uporabe nezadostnih varnostnih rešitev (npr.: slaba avtorizacija in avtentikacija, slab nadzor nad strežniško infrastrukturo, slaba programska oprema za kriptiranje, slab nadzor nad potmi prenašanja podatkov, slabo varovanje arhiviranih podatkov itn.).

Ob uresničitvi grožnje in posledičnem varnostnem incidentu je treba mobilno napravo ustrezno zavarovati in zbrati ter pregledati dokaze, ki so nastali. Uveljavljanje pravne odgovornosti ter preiskovanje mobilne naprave je odvisno od vrste podatkov, ki so na mobilni napravi. Za uspešno uveljavljanje pravne odgovornosti, pa tudi zgolj za praktično omejevanje škode znotraj in zunaj organizacije zaradi napada na mobilno napravo, je nujen predpogoj prijava varnostnega incidenta – to je lahko prijava službam znotraj organizacije ali omenjenim, zato pristojnim organom zunaj organizacije.

V primeru uresničitve grožnje je mogoč kazenski postopek, saj lahko ravnanje grožnje ustreza posamezni definiciji kaznivega dejanja iz Kazenskega zakonika (KZ-1, 2008). V tem primeru je mogoč zaseg in pregled mobilne naprave v skladu z Zakonom o kazenskem postopku (ZKP, 1994). Ker Ustava Republike Slovenije (1991) s 37.[2] in 38.[3] členom uporabniku mobilne naprave zagotavlja komunikacijsko in informacijsko varstvo podatkov na mobilni napravi, lahko poteka zaseg in pregled elektronske naprave v kazenskem postopku le v skladu z določili ZKP (1994). Poleg tega tudi KZ-1 (2008) s 139. (kršitev tajnosti občil) in 143. členom (zloraba osebnih podatkov) posredno varuje uporabnike mobilnih naprav, saj je z omenjenimi členi vsak nezakoniti poseg v zasebnost uporabnika (in to je tudi nezakonit pregled ali odvzem posameznikove mobilne naprave) in s tem zloraba osebnih podatkov lahko smatrana kot kaznivo dejanje, če so izpolnjeni zakonski znaki teh kaznivih dejanj, torej tudi v primeru zasega in pregleda mobilne naprave v nasprotju z določili ZKP (1994).

Zaseg in preiskava elektronske naprave, med katere spadajo tudi mobilne naprave, sta urejena v 219.a in 223.a členu ZKP (1994). Preiskava nosilcev elektronskih podatkov se tako lahko opravi, če so podani utemeljeni razlogi za sum, da je bilo storjeno kaznivo dejanje in je podana verjetnost, da elektronska naprava vsebuje elektronske podatke, na podlagi katerih je mogoče osumljenca ali obdolženca identificirati, odkriti ali prijeti ali odkriti sledove kaznivega dejanja, ki so pomembni za kazenski postopek, ali jih je mogoče uporabiti kot dokaz v kazenskem postopku. Za preiskavo policija potrebuje:

- vnaprejšnjo pisno privolitev imetnika ter vseh policiji znanih in dosegljivih uporabnikov elektronske naprave, ki na njej utemeljeno pričakujejo zasebnost (uporabnik), ali
- obrazloženo pisno odredbo sodišča.

Imetnik oziroma uporabnik elektronske naprave mora omogočiti dostop do naprave, predložiti šifrirne ključe oziroma šifrirna gesla in pojasnila o uporabi naprave, ki so potrebna, da se doseže namen preiskave. Če noče tako ravnati,

2 *37. člen Ustave RS (1991) (varstvo tajnosti pisem in drugih občil): »Zagotovljena je tajnost pisem in drugih občil. Samo zakon lahko predpiše, da se na podlagi odločbe sodišča za določen čas ne upošteva varstvo tajnosti pisem in drugih občil in nedotakljivost človekove zasebnosti, če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države.«*

3 *38. člen Ustave RS (1991) (varstvo osebnih podatkov): »Zagotovljeno je varstvo osebnih podatkov. Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja. Zbiranje, obdelovanje, namen uporabe, nadzor in varstvo tajnosti osebnih podatkov določa zakon. Vsakdo ima pravico seznaniti se z zbranimi osebnimi podatki, ki se nanašajo nanj, in pravico do sodnega varstva ob njihovi zlorabi.«*

ga smemo kaznovati oziroma zapreti, dokler ne sodeluje oziroma maksimalno 1 mesec, razen če gre za osumljenca ali obdolženca ali osebo, ki ne sme biti zaslišana kot priča ali se je v skladu z zakonom odrekla pričevanju. Preiskavo opravi strokovno usposobljena oseba (ZKP, 1994: 219.a čl.), pred preiskavo pa se morajo podatki v elektronski obliki zavarovati tako, da se shranijo na drug ustrezen nosilec podatkov na način, da se ohrani istovetnost in integriteta podatkov ter možnost njihove uporabe v nadaljnjem postopku ali se izdela istovetna kopija celotnega nosilca podatkov, pri čemer se zagotovi integriteta kopije teh podatkov. Če to ni mogoče, se elektronska naprava zapečati, če je le mogoče, zgolj tisti del elektronske naprave, ki naj bi vseboval iskane podatke (ZKP, 1994: 223.a čl.). Pri zavarovanju podatkov se v zapisnik zapišejo kontrolne vrednosti oziroma se na drug ustrezen način v zapisniku zagotovi možnost naknadnega preverjanja istovetnosti in integritete zavarovanih podatkov. Pri tem je treba biti pozoren tudi na vsebino podatkov, saj je dokazano, da zgolj kontrolna vrednost za zagotavljanje ni dovolj. Kopije zaseženih podatkov se hranijo, dokler je to potrebno za postopek (ZKP, 1994: 223.a čl.). Z vidika zagotavljanja integritete zavarovanih podatkov je tudi pri elektronskih dokazih z mobilne naprave pomembna t. i. skrbniška veriga (angl. *chain of custody*). V skladu z zakonodajo in pravilnostjo postopka se razčlenijo koraki preiskovanja incidenta in zavarovanja dokazov. Po incidentu sledi preiskava. V tem trenutku se začne skrbniška veriga, s katero se zagotovi integriteta in celovitost dokazov (Šavnik, 2007). Izvedejo se forenzični postopki in jasno določena revizijska sled forenzičnih postopkov. Zaključek preiskave je poročilo o ugotovitvah, na podlagi katerega so iz pravnega vidika mogoči tako kazenski kot civilni pravni postopki.

Enako stroga je ureditev zasega in pregleda mobilne naprave zunaj kazenskega postopka (na primer znotraj delovne organizacije). Zaseg in pregled mobilne naprave morata biti skladna z Zakonom o varstvu osebnih podatkov (ZVOP-1, 2004), v katerem je opredeljena raba in obdelava osebnih podatkov, saj so na mobilni napravi praktično vedno tudi osebni podatki. Le v takem primeru sme organizacija preiskati mobilno napravo druge osebe, tudi svojega zaposlenega, ne da bi kršila ZVOP-1 (2004) in s tem izvršila kaznivo dejanje iz 139. in 143. člena KZ-1 (2008) ter se izpostavila tako kazenski kot tudi odškodninski odgovornosti. Takšno je tudi stališče slovenskega Informacijskega pooblaščenca (2014). Zaseg in pregled mobilne naprave v zasebnem sektorju je tako v skladu z ZVOP-1 (2004: 8. čl.) mogoč le s predhodnim soglasjem uporabnika ali pa na podlagi zakona, v praksi torej le izjemoma – npr. če tako nalaga zakon ali posebne izredne okoliščine (na primer smrt delavca), pri tem pa je nujno treba upoštevati načelo sorazmernosti.

Da bi ugotovili potrebe po pregledu in dejanski forenzični preiskavi mobilne naprave ter za to skladno z zakonom zagotovili ustrezne akte (pravilnike in standarde) v podjetjih, smo izvedli raziskavo, ki odkriva načine uporabe mobilnih naprav med zaposlenimi v različnih organizacijah, obstoječe elemente varovanja in formalno urejenost področja.

4 METODE

Med slovenskimi organizacijami je bila izvedena dvostopenjska raziskava, ki je zaposlene in predstavnike posamezne organizacije, odgovorne za varno rabo

mobilnih naprav med zaposlenimi v posamezni organizaciji, spraševala o načinih rabe mobilnih naprav med zaposlenimi, vključno s podatki, ki jih hranijo na mobilni napravi in o načinih zagotavljanja celovite kibernetske varnosti. Cilji raziskave so bili pridobiti informacije o načinih vpeljave in rabe tako tehničnih kot organizacijskih zaščit pri rabi mobilnih naprav med zaposlenimi v posamezni organizaciji.

Prvi del raziskave smo izvedli s pomočjo spletnega vprašalnika, ki je bil v času od maja 2012 do februarja 2013 objavljen na spletnem portalu »1ka« (www.1ka.si). Na spletni vprašalnik je v tem času odgovorilo nekaj več kot 600 uporabnikov mobilnih naprav iz 34 različnih organizacij v Sloveniji. Skoraj polovica vprašalnikov je bila izpolnjena nepopolno, zato smo jih izločili iz nadaljnje analize. Zaradi tega rezultatske tabele prikazujejo število respondentov »*N*« na posamezno vprašanje, iz njega pa so izvedeni tudi deleži.

Drugi del raziskave smo izvedli z izvedbo 22 intervjujev z osebami, ki so v organizacijah odgovorne za rabo mobilnih naprav med zaposlenimi. Vprašanja so bila preko elektronske pošte posredovana predstavnikom 34 organizacij, kjer so zaposleni odgovarjali o rabi mobilnih naprav v prvem delu raziskave. Pri pripravi vodilnih vprašanj odprtega tipa (19 vprašanj) smo sledili teoretičnim izhodiščem o rabi mobilnih naprav. S tem smo od strokovnjakov pridobili informacije o njihovih izkušnjah in pogledih na rabo mobilnih naprav v njihovih organizacijah, urejanju področja in možnostim preiskovanja in pregona v primeru uresničitve groženj.

V prvem delu raziskave smo ugotavljali način rabe mobilnih naprav. Strukturo podjetij, ki so odgovarjali na vprašanja, prikazuje tabela 1.

Tabela 1: Odstotek anketirancev po velikosti organizacije

Odgovori	***N***	**%**
0–9 (mikropodjetje)	7	2
10–49 (majhno podjetje)	23	8
50–249 (srednje veliko podjetje)	26	9
250+ (veliko podjetje)	248	81
Skupaj	304	100

V tabeli 1 je prikazano, da največji odstotek ljudi, ki so odgovarjali na vprašanja, prihaja iz velikih podjetij; teh je bilo 81 odstotkov, deleži anketirancev iz preostalih velikosti podjetij so bili manjši. Iz mikropodjetij sta bila dva odstotka vprašanih, iz majhnih podjetij osem odstotkov in iz srednje velikih podjetij devet odstotkov. Razmerje med velikostjo podjetja in številom uporabnikov, ki so odgovarjali na spletno anketo, je razumljivo. Večje, ko je podjetje, več ljudi lahko odgovarja na anketo in posledično sta večja frekvenca in delež. V nadaljevanju bo pri nekaterih rezultatih iz raziskave, ki bodo poudarjeni v razlagi, razvidna razlika med delovanjem posameznikov in organizacije pri zagotavljanju informacijske varnosti in varno rabo mobilnih naprav. Izobrazbeno strukturo udeležencev predstavlja tabela 2.

Tabela 2: Izobrazba, sodelujočih v anketi

Odgovori	*N*	%
Osnovna šola	3	1
Srednja šola	57	19
Višja, visoka, univerzitetna izobrazba	200	65
Magisterij, doktorat	46	15
Skupaj	306	100

Največ anketirancev je končalo višjo, visoko ali univerzitetno stopnjo študija (65 odstotkov), 19 odstotkov jih je imelo srednješolsko izobrazbo, 15 odstotkov pa jih je imelo magisterij ali doktorat. Glede na rezultate v tabeli trdimo, da so med izpraševanci ljudje s stopnjo izobrazbe, ki jim omogoča dovolj visoko razgledanost in znanje, da lahko prepoznavajo grožnje rabi mobilnih naprav, vrednost posledic ob uresničitvi groženj in pomen rabe varnostnih zaščit.

5 REZULTATI RAZISKAVE

V tabeli 3 je prikazano, s kakšnim namenom zaposleni v sodelujočih organizacijah uporabljajo mobilne naprave, nameščeno programsko opremo in uporabo različnih storitev.

Tabela 3: Namen rabe mobilne naprave

Uporabljene storitve	Delo	Zasebno	Delo in zasebno	*N* %
Prenos elektronske pošte	201	187	143	245
	82 %	76 %	58 %	79 %
Brskanje po spletu	138	230	124	244
	57 %	94 %	51 %	79 %
Opravljanje službenih obveznosti (od doma)	174	49	37	186
	94 %	26 %	20 %	60 %
Cestna navigacija	82	172	70	184
	45 %	93 %	38 %	60 %
Opravljanje službenih obveznosti (na delovnem mestu)	160	30	26	164
	98 %	18 %	16 %	53 %
Poslušanje glasbe, igranje iger ali gledanje videoposnetkov na internetu	13	129	13	129
	10 %	100 %	10 %	42 %
Prenos podatkov, datotek z interneta	62	112	45	129
	48 %	87 %	35 %	42 %
Predvajanje glasbe in filmov	10	123	8	125
	8 %	98 %	6 %	40 %
Uporaba različnih programov za razvedrilo	9	121	8	122
	7 %	99 %	6 %	39 %

Tabela 3: Nadaljevanje

Uporabljene storitve	Delo	Zasebno	Delo in zasebno	*N* %
Branje e-knjig in člankov	47	108	41	114
	41 %	95 %	36 %	37 %
Dostop do spletnih socialnih omrežij (Facebook, Twitter, Google+ itn.)	19	111	16	114
	17 %	97 %	14 %	37 %
Prenos različnih programov z interneta	39	100	33	106
	37 %	94 %	31 %	34 %
Igranje iger	10	99	5	104
	10 %	95 %	5 %	34 %
Uporaba različnih programov za delo	64	69	34	99
	65 %	70 %	35 %	32 %
Internetna komunikacija (instantmessaging – MSN, Skype, Voip itn.)	34	87	27	94
	36 %	93 %	29 %	30,4 %
Izmenjava poslovnih podatkov	85	20	15	90
	94 %	22 %	16 %	29 %
Povezovanje s poslovnim sistemom organizacije	63	15	10	68
	93 %	22 %	15 %	22 %
Urejanje besedila in podatkov (Word, Excel, Access itn.)	49	42	26	65
	75 %	65 %	40 %	21 %
E-bančništvo, plačevanje računov	8	56	5	59
	14 %	95 %	9 %	19 %
Shranjevanje dokumentov na spletnem mestu (Dropbox, GDrive, SkyDrive ipd.)	12	57	11	58
	21 %	98 %	19 %	19 %
Spletno nakupovanje	1	48	1	48
	2 %	100 %	2 %	16 %

Na vprašanje je odgovorilo 310 izpraševancev. Izpraševanci so lahko istočasno izbrali več ponujenih odgovorov (v tabeli 3 navedenih storitev, ki jih uporabnik lahko uporablja na mobilni napravi), v okviru teh pa eno od dveh razdelitev ali obe. Stolpec *N* (v odstotkih) v tabeli predstavlja število in odstotek vseh izpraševancev (od celote tistih, ki so odgovorili na vprašanje), ki so izbrali posamezno spremenljivko. Primer: anketiranec je lahko označil več storitev ali vse, ki jih uporablja na svoji mobilni napravi, ter s kakšnim namenom uporablja mobilno napravo (za osebne in/ali poslovne namene). Največ jih je odgovorilo, da uporabljajo mobilno napravo za prenos/prejetje elektronske pošte (79 odstotkov od 310 izpraševancev). Zanimivo je, da jih 82 odstotkov (od predhodnih 79 odstotkov, ki je v tem primeru celota) uporablja storitev prenosa elektronske pošte v okviru svojih delovnih nalog, 76 odstotkov pa tudi za zasebne namene; 58 odstotkov jih storitev prenosa elektronske pošte uporablja tako med delom kot tudi zasebno. Iz rezultatov je razvidno, da je mešanje osebne in poslovne rabe pogosto. Storitev opravljanja službenih obveznosti doma je potrdilo 186 (60

odstotkov) od 310 izpraševancev, kar pomeni, da mobilno napravo v omenjenem odstotku uporabljajo za službene namene tudi doma.

Od teh 186 jih 175 (94 odstotkov) omenjeno storitev uporablja izključno za delo, 48 (26 odstotkov) pa tudi za zasebno dejavnost. Rezultati torej jasno pokažejo, da imajo uporabniki mobilnih naprav na svojih mobilnih napravah tudi (svoje) osebne podatke. To je pomembno z vidika zaščite posameznika v skladu ZVOP-1 (2004) v primeru, da organizacija želi zaseči in pregledati službeno mobilno napravo.

Glede na podatke iz tabele 3 in omenjena dejstva o zaznanih uresničenih grožnjah med uporabniki mobilnih naprav ugotavljamo, da pri rabi mobilnih naprav in uresničitvi groženj vedno obstaja tveganje izgube podatkov. Ob uresničitvi grožnje je pomembno, da uporabnik incident takoj prijavi pristojnim in s tem zmanjša količino izgubljenih podatkov. Izpraševalcem smo postavili vprašanje, komu prijavljajo zaznane incidente.

Tabela 4: Organi, ki so najpogosteje obveščeni o zaznanih zlorabah

Organi, ki jim ob incidentu prijavimo zlorabo	***N* (293)**	**%**
Tisti, ki v organizaciji skrbi za mobilne naprave, računalnike	203	69
Ponudnik mobilne telefonije (Mobitel, SiMobil, Tuš idr.)	170	58
Služba, ki je v organizaciji zadolžena za odpravljanje napak na informacijskih sistemih in ima navodila, kako ravnati ob izgubi ali kraji mobilne naprave	132	45
Policija	127	43
Nihče, saj na mobilni napravi nimam pomembnih podatkov	19	6
Nihče, ker lahko oddaljeno izbrišem podatke	10	3
SI-CERT (Slovenian Emergency Response Team) idr.	7	2
Nikomur, vseeno mi je	2	1

Pri tem smo želeli ugotoviti, kateri od naštetih oseb, organov ali organizacij bi uporabnik prijavil zlorabo mobilne naprave. Izpraševanci so lahko istočasno izbrali več ponujenih odgovorov. Na vprašanje je odgovorilo 293 izpraševancev. Največ jih je izbralo prvo možnost, torej bi zlorabo mobilne naprave prijavili tistemu, ki v organizaciji skrbi za mobilne naprave in računalnike (69 odstotkov od 293 izpraševancev). Pomembno je, da ima organizacija pravilnik, politiko ali standard, ki obligatorno določa, kako ravnati v takih primerih. Vsebino pravilnika morajo poznati vsi zaposleni. Oseminpetdeset odstotkov uporabnikov bi obvestilo tudi ponudnika mobilne telefonije. Skrb vzbujajoč je podatek, da odstotek uporabnikov ne bi naredilo ničesar.

Odgovornim osebam za rabo mobilnih naprav v posameznih organizacijah smo v sklopu intervjujev zastavili vprašanje: *Ali imate v organizaciji posebne pravilnike o varni rabi mobilnih naprav? Katere elemente varnosti vsebujejo?* Štiri (18,2 %) organizacije imajo pravilnike varne rabe mobilnih naprav. Zaskrbljujoč je podatek, da 81,8 % organizacij pravilnikov o varni rabi mobilnih nima. Kar pomeni, da tudi postopkov, ki sledijo po ZVOP-1 (2004) in se dotikajo mobilnih naprav in osebnih podatkov, nimajo. Tovrstni pravilniki so pomembni tudi zato, ker se v njih opredeljuje, kako ukrepati v primeru informacijskovarnostnega incidenta.

6 RAZPRAVA IN ZAKLJUČKI

Stopnja tveganja rabe storitev na mobilni napravi, ki smo jih predstavili, je odvisna predvsem od groženj, ki so jim naprave in storitve izpostavljene in pogostost že uresničenih groženj. V primeru varnostnih incidentov mora organizacija sprejeti vse ukrepe, da zagotovi, da se enak ali primerljiv primer ne bi več ponovil. Zato smo v raziskavi pri vprašanju »Pri rabi mobilnih napravi se mi lahko zgodi« omogočili možnost izbire »Se mi je že zgodila«. Podatki iz raziskave pokažejo, da je 8 odstotkov izpraševancev že doživelo odtujitev mobilne naprave, 2 odstotka oddajanje podatkov brez njihove vednosti in po 1 odstotek je tistih, ki so že doživeli krajo podatkov, sledenje (posledica nenadzorovanega oddajanja GPS-modula) ali okužba z zlonamerno kodo (*malware*, *spyware*, virusi, trojanski konji itn.). To so seveda samo podatki, kjer so bile grožnje oz. zlorabe zaznane. Pojavlja se vprašanje, koliko je takih uresničitev groženj, ki jih uporabniki niso zaznali. Dejstvo o redki rabi pravilnikov, ki določajo način varne rabe mobilnih naprav v organizacijah, smo potrdili tudi z drugim delom raziskave. Kot smo omenili, je v primeru varnostnega incidenta priporočljivo obvestiti pristojne organe, da se izvede bodisi zaseg in pregled mobilne naprave v kazenskem postopku po ZKP (1994) bodisi pregled mobilne naprave v zasebnem sektorju v skladu z ZVOP-1 (2004). S tem se zavarujeta izvirnost in integriteta pridobljenih digitalnih dokazov ter postopa skladno z zakonodajo. Prijava varnostnega incidenta pristojnim organom je priporočljiva, vprašanje pa je, ali za to obstaja dolžnost. Pravna dolžnost obstaja zgolj v primeru, da je v primeru opustitve prijave predpisana sankcija.

V okviru kazenskega prava tako govorimo o kaznivem dejanju opustitve ovadbe, ki pa ga vsakdo lahko izvrši le v primeru opustitve ovadbe najhujših kaznivih dejanj (zagrožena kazen petnajst let ali več zapora) (KZ-1, 2008: 281. čl.), kar bo v primeru varnostnega incidenta z mobilno napravo redko.[4] Strožjo dolžnost imajo le uradne osebe, ki zavestno opustijo ovadbo kaznivega dejanja, za katero zvejo pri opravljanju svoje službe (če je za izvedeno kaznivo dejanje zagrožena kazen tri leta ali več zapora) (KZ-1, 2008: 2. odst., 281. čl.), in pa državni organi in organizacije z javnimi pooblastili (kazniva dejanja, za katera se storilec preganja po uradni dolžnosti, če so o njih obveščeni ali če kako drugače zvedo zanje) (ZKP, 1994: 145. čl.). Dolžnost prijaviti varnostni incident pod grožnjo kazenske odgovornosti za tako opustitev bo tako znotraj zasebnega sektorja redka. Možna pa je odškodninska odgovornost po delovni in splošni obligacijski zakonodaji, če zaradi opustitve prijave varnostnega incidenta nastane nadaljnja škoda, ob izpolnjenih vseh predpostavkah odškodninske odgovornosti (Obligacijski zakonik, 2001; Zakon o delovnih razmerjih [ZDR-1], 2013), obenem pa disciplinska odgovornost.

V povezavi z disciplinsko odgovornostjo, ki bi uporabnike mobilnih naprav posredno *silila*, da prijavljajo varnostne incidente, je pomembno, da imajo organizacije pravilnike, ki opredeljujejo način rabe mobilnih naprav in zahtevane postopke ob varnostnem incidentu, vključno z možnostjo pregleda mobilne naprave in dolžnostjo prijave varnostnega incidenta ter sankcijo ob opustitvi le-te.

4 *Taka sankcija je namreč po KZ-1 (2008) zagrožena praviloma za umor in določena kazniva dejanja zoper človečnost.*

Vsebina mora slediti določilom ZVOP-1 (2004), kjer je opredeljena raba in obdelava osebnih podatkov, saj mobilne naprave vsebujejo osebne podatke. Teh, kot izhaja iz rezultatov raziskave, imajo uporabniki veliko. Obravnavanje incidenta in nadaljnje preiskovanje, bodisi v zasebnem sektorju bodisi v kazenskem postopku, pa mora potekati v skladu z zakonodajo in pravilnikom, v nasprotnem primeru so dokazi v kazenskem postopku nezakoniti in jih je treba izločiti (ZKP, 1994: 219.a čl.), v zasebnem sektorju pa se organizacija, ki je izvedla nezakonit poseg, izpostavi odškodninski, prekrškovni in tudi kazenski odgovornosti.

Rezultati predstavljene raziskave kažejo na velik porast rabe mobilnih naprav pri številnih poslovnih opravilih. Mešanje osebnih in poslovnih potreb ter dostopa do podatkov postaja v kibernetskem prostoru stalnica. Tako se povečuje tveganje zlorab, saj se (kot je razvidno iz raziskav organizacij McAfee (2014) in Juniper Networks (2013)) število groženj dnevno povečuje. Organizacije kljub temu ne pristopajo k zaščiti podatkov s pomočjo pravilnikov, politik in standardov, le-ti pa so osrednjega pomena z več vidikov – zagotavljanje varne rabe mobilnih naprav med uporabniki ter morebitno ustrezno preiskovanje varnostnega incidenta ob rabi mobilne narave kot posledica uresničitve groženj. Rezultati raziskave kažejo, da imajo uporabniki mobilnih naprav na eni mobilni napravi tako poslovne kot tudi osebne podatke, tako da je kakršno koli pregledovanje mobilne naprave znotraj zasebnega sektorja oziroma organizacije podvrženo ureditvi ZVOP-1 (2004). Zato je pomembno, da je tak pregled predviden v pravilnikih posamezne organizacije. Ker lahko varnostni incident z mobilno napravo predstavlja podlago za uvedbo kazenskega postopka in pregled naprave v kazenskem postopku, je treba s pravilnikom urediti postopek ravnanja ob varnostnem incidentu in morebitno dolžnost prijave le-tega. Rezultati kažejo, da določene organizacije temu sledijo, da pa obstaja še veliko prostora za izboljšave na tem področju. S tem se izboljša učinkovitost kazenskega postopka v primeru kaznivih dejanj, dokazi se hitreje zavarujejo, s tem pa se zmanjša temno polje izvajanja kibernetske kriminalitete.

Raba poslovnih mobilnih naprav za poslovne in zasebne namene je dejstvo, ki ga delodajalci dopuščajo. Zaradi tega je treba ob informacijskovarnostnih incidentih upoštevati tudi pravico do pričakovane zasebnosti, razen v primerih, ko se le-te uporabnik ne odreče vnaprej s podpisom strinjanja preiskave, ki jo opredeljujejo informacijskovarnostne politike. Ker pričakujemo naraščanje različnih incidentov, povezanih z mobilnimi napravami, je v organizacijah potrebna ustrezna priprava ali dopolnitev informacijskovarnostnih politik in dosledno uresničevanje predpisanih preventivnih ukrepov. Tako bodo podatki manj ogroženi, potreba po preiskovanju incidentov pa bistveno manjša.

UPORABLJENI VIRI

Bernik, I. (2014). *Cybercrime and cyberwarfare.* London: ISTE; Hoboken: Wiley.

Europol. (2013). *Socta 2013: EU serious and organised crime threat assessment*. Pridobljeno na https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

F-Secure. (2013). *Mobile threat report, 2013.* Pridobljeno na http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf

Gartner. (2013). *Gartner says worldwide PC, tablet and mobile phone shipments to grow 5.9 percent in 2013 as anytime-anywhere-computing drives buyer behavior*. Pridobljeno na http://www.gartner.com/newsroom/id/2525515

Informacijski pooblaščenec. (2014). *Vse več prekrškov zaradi nezakonitih vpogledov v e-pošto delavcev*. Pridobljeno na https://www.ip-rs.si/novice/detajl/vse-vec-prekrskov-zaradi-nezakonitih-vpogledov-v-e-posto-delavcev/?cHash=a3bbe1883a9d914f5aab7c822a94bbdd

International Data Corporation [IDC]. (2013). *Annual report to members.* Pridobljeno na http://www.idc.org/pdf/13_ici_annual.pdf

International Telecommunication Union [ITU]. (2012). *Measuring the information society*. Pridobljeno na http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf

Juniper Networks. (2013). *Juniper Networks third annual mobile threats report: March 2012 through March 2013*. Pridobljeno na http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf

Kazenski zakonik [KZ-1]. (2008). *Uradni list RS*, (55/08 in spremembe).

Lookout. (2011). *Lookout mobile threat report.* Pridobljeno na https://www.lookout.com/static/ee_images/lookout-mobile-threat-report-2011.pdf

McAfee. (2014). *McAfee labs 2014 threats predictions*. Pridobljeno na http://www.mcafee.com/uk/resources/reports/rp-threats-predictions-2014.pdf

Norton, K. (2012). *Mobile security: 6 reasons devices remain vulnerable*. Pridobljeno na http://deloitte.wsj.com/cio/2012/10/24/mobile-security-6-reasons-devices-remain-vulnerable/

Obligacijski zakonik. (2001). *Uradni list RS*, (83/01 in spremembe).

Olavsrud, T. (2013). *Mobile attacks top the list of 2013 security threats*. Pridobljeno na http://www.cio.com/article/725948/Mobile_Attacks_Top_the_List_of_2013_Security_Threats

Open Web Application Security Project [OWASP]. (2013). *OWASP mobile security project*. Pridobljeno na https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Šavnik, J. (2007). Kaznivo dejanje vdora v informacijski sistem po 242. členu kazenskega zakonika. *Varstvoslovje, 9*(1/2), 117–124.

Ustava Republike Slovenije. (1991). *Uradni list RS*, (33/91-I in spremembe).

Zakon o delovnih razmerjih [ZDR-1]. (2013). *Uradni list RS*, (21/13 in spremembe).

Zakon o kazenskem postopku [ZKP]. (1994). *Uradni list RS*, (63/1994 in spremembe).

Zakon o varstvu osebnih podatkov [ZVOP-1]. (2004). *Uradni list RS*, (86/04 in spremembe).

O avtorjih:

Dr. Blaž Markelj, predavatelj za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: blaz.markelj@fvv.uni-mb.si

Dr. Igor Bernik, izredni profesor za informacijsko varnost, predstojnik Katedre za informacijsko varnost na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: igor.bernik@fvv.uni-mb.si